

Permutation Groups, Complexes, and Rearrangeable Connecting Networks

By V. E. BENEŠ

(Manuscript received March 12, 1964)

In the interest of providing good telephone service with efficient connecting networks, it is desirable to have at hand a knowledge of some of the combinatorial properties of such networks. One of these properties is rearrangeability: a connecting network is rearrangeable if its permitted states realize every assignment of inlets to outlets, or alternatively, if given any state x of the network, any inlet idle in x , and any outlet idle in x , there is a way of assigning new routes (if necessary) to the calls in progress in x so that the idle inlet can be connected to the idle outlet.

A natural algebraic and combinatorial approach to the study of rearrangeable networks is described, with attention centered principally on two-sided networks built of stages of square crossbar switches, each stage having N inlets and N outlets. The approach is based in part on the elementary theory of permutation groups. The principal problem posed (and partly answered) is this: What connecting networks built of stages are rearrangeable? Sufficient conditions, including all previously known results, are formulated and exemplified.

1. INTRODUCTION

A connecting network is an arrangement of switches and transmission links through which certain terminals can be connected together in many combinations. Typical examples of connecting networks can be found in telephone central offices, where they are used to complete calls among the customers themselves, and between customers and outgoing trunks leading to other offices.

In the interest of providing good service with efficient connecting networks, it is desirable to have a thorough understanding of some of the combinatorial properties of such networks. In a previous paper,¹ we singled out three such combinatory properties as useful in assessing the performance of connecting networks. The weakest of these properties

was that of *rearrangeability*. A connecting network is rearrangeable if its permitted states realize every assignment of inlets to outlets, or alternatively, if given any state x of the network, any inlet idle in x , and any outlet idle in x , there is a way of assigning new routes (if necessary) to the calls in progress in x so as to lead to a new state of the network in which the idle inlet can be connected to the idle outlet.

Figs. 1 and 2 show the structure of two connecting networks built out of square crossbar switches, with each switch capable of connecting any subset of its inlets to an equinumerous subset of its outlets in any desired one-one combination. The network of Fig. 1 is often found in telephone central offices; we may call it the No. 5 crossbar network. It is *not* rearrangeable. The network of Fig. 2 *is* rearrangeable, but so far it has not found extensive practical use.

We shall describe a natural algebraic and combinatorial approach to the study of rearrangeability. For the most part we restrict attention to two-sided connecting networks that are built of stages of crossbar switches, and have the same number N of inlets as outlets. The approach is based in part on the elementary theory of permutation groups. The way the connection with group theory arises can be summarized as follows: a maximal state of the network is one in which no additional

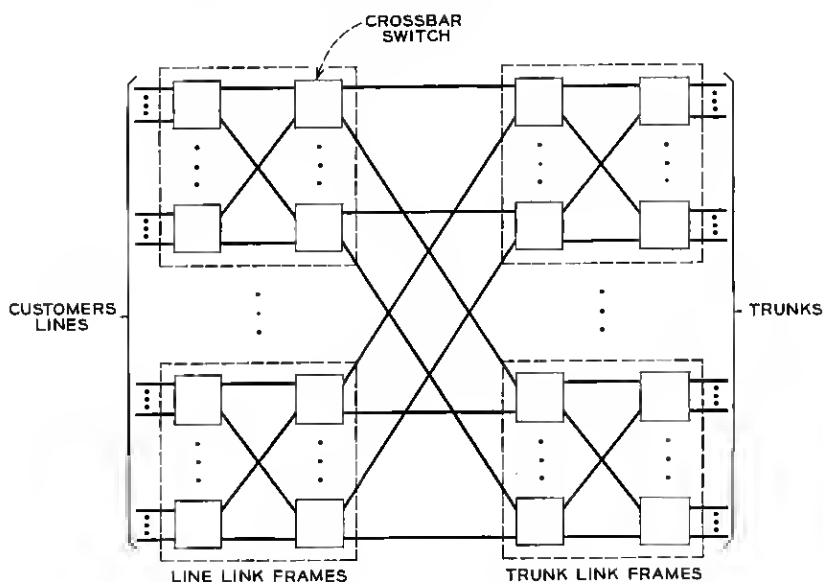


Fig. 1 — Structure of No. 5 crossbar network.

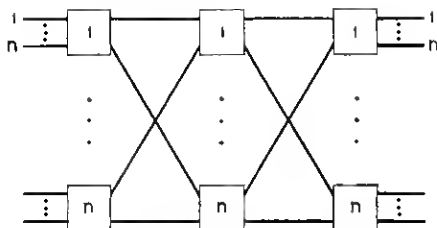


Fig. 2 — Rearrangeable network.

calls can be completed in the network; suppose that both the inlets and the outlets are numbered in an arbitrary way from 1 to N ; each maximal state realizes some submap of a permutation on $\{1, \dots, N\}$; the network is rearrangeable if and only if the whole group of all permutations of $\{1, \dots, N\}$ is generated in this way by the maximal states of the network. Details are worked out in the main body of the paper.

It is not possible to explore in one paper all the possible uses of group theory in the study of connecting networks. Indeed, we shall restrict ourselves to formulating the fundamental problem of rearrangeable networks in terms of complexes of permutations, and to giving a partial answer. One of the difficulties with the approach is that it always seems to be easier to obtain results about groups by the few available methods known for rearrangeable networks, than *vice versa*.

A sequel² to the present paper is concerned with the problem of synthesizing a rearrangeable network (for N inlets and outlets), subject to certain structural conditions and to the condition that it have a minimum number of crosspoints.

II. SUMMARY

In Section III we define a precise general notion of a "stage" of switching in a connecting network, and, after describing how the networks which will be of interest are built out of stages by joining them together by patterns of links, we pose two problems: first, to discover what networks built in this way are rearrangeable; and second, to synthesize optimal rearrangeable networks of given size, optimal in the sense of having fewest crosspoints (among those in some class of networks having practical interest). (See Ref. 2.)

Section IV is devoted to giving a formulation of the first problem (discovering rearrangeable networks) in terms of partitions and permutation groups, using the notion of stage. In Section V we discuss how stages

generate complexes (in the group theory sense, i.e., sets of group elements). It is shown that a stage can generate a subgroup only if it contains a substage made of square switches, a result that indicates to some extent the "best possible" nature of stages made of square switches.

A known example, discussed in Section VI, indicates how a particular symmetric group S is generated by a rearrangeable network in the form

$$S = \left\{ \prod_{i=1}^3 \varphi_i \right\}$$

with φ_1, φ_3 in a subgroup H and φ_2 in a certain subgroup $\varphi^{-1}H\varphi$ conjugate to H .

The remainder of the paper is devoted to proving two "rearrangeability" theorems for connecting networks built of stages of square switches. The first theorem gives sufficient conditions under which a set of stages of square switches connected by link patterns will give rise to a rearrangeable network. The second theorem indicates a simple way of describing link patterns and stages that satisfy the hypotheses of the first theorem, and so yield many specific rearrangeable networks, generalizations of those given by Paull.³

III. STAGES AND LINK PATTERNS

The switches in Figs. 1 and 2 are arranged in columns which we shall call *stages*, the switches in these stages being identical. Two adjacent stages are connected by a pattern of *links* or *junctors*. Along with the switches, the link patterns are responsible for the distributive characteristics of the network. They afford an inlet ways of reaching many outlets. Obviously, each outlet on a switch in a given stage is some inlet of the next stage, if there is one. Suppose that the N inlets are numbered in an arbitrary way, and that the N outlets are also numbered in an arbitrary way, both from 1 to N . Then it is clear that each link pattern, and each permitted way of closing the largest possible number of cross-points in a stage, viz. N , can be viewed abstractly as a permutation on $\{1, \dots, N\}$. Both the networks in Figs. 1 and 2 have the property that all maximal* states have the same number N of calls in progress, and any such maximal state realizes a permutation which is a *product* of certain of the permutations represented by the link patterns and the stages.

It will be convenient to generalize the usual notion of a "stage" of switching in a connecting network. By a stage (of switching) we shall

* I.e., states in which no additional calls can be completed.

mean a connecting network constructed as follows: with I the set of inlets, and Ω that of outlets, we choose an arbitrary subset S of $I \times \Omega$, and we place a crosspoint between all and only those inlets $u \in I$ and outlets $v \in \Omega$ such that $(u, v) \in S$. We shall also speak of S itself as the "stage." Thus we make

Definition 1: A stage is a subset of $I \times \Omega$.

This terminology is easily seen to be an extension of the usual one, according to which, e.g., a column of switches in Fig. 1 forms a stage, the network having four stages separated (or joined) by three link patterns. Actually, a link pattern may be associated with one or the other (but usually not both) of the stages it connects, to define a new stage; we do not usually do this.

Definition 2: A stage S is made of square switches if and only if there is a partition Π of $\{1, \dots, N\}$ such that

$$S = \bigcup_{A \in \Pi} (A \times A).$$

Definition 3: A substage S' of S is a subset of S .

Except in the trivial case in which S is actually a square N -by- N switch (i.e., $S = I \times \Omega$), a stage S will not by itself give rise to a rearrangeable network. Still, it is known that several stages joined end to end by suitable link patterns can together give rise to such a network, e.g., that of Fig. 2. We can thus formulate two fundamental questions about connecting networks built out of stages:

(1) What stages and link patterns can be used to construct a rearrangeable network?

(2) What stages, and how many of them, should be used to construct a rearrangeable network that has a minimum number of crosspoints (switches) for a given number of terminals on a side?

Question (1) is studied in the present work, while question (2) is treated in another paper.²

IV. GROUP THEORY FORMULATION

We shall adopt some notational conventions from group theory to simplify our presentation. Let G be a group. It is customary to speak of a subset $K \subseteq G$ as a *complex*. If $x \in G$, then xK denotes the set of products xy with $y \in K$, Kx denotes the set of products yx with $y \in K$. Similarly, if K_1 and K_2 are complexes, K_1K_2 denotes the set of products yz with $y \in K_1$ and $z \in K_2$.

A group G of permutations is called *imprimitive*⁴ if the objects acted

on by the permutations of G can be partitioned into mutually disjoint sets, called the sets of *imprimitivity*, such that every $\varphi \in G$ either permutes the elements of a set among themselves, or carries that set onto another. That is, there is a nontrivial partition Π of the set X of objects acted on such that $\varphi \in G$ and $A \in \Pi$ imply $\varphi(A) \in \Pi$. We shall extend this terminology as follows:

Definition 4: G is called *strictly imprimitive* if it is imprimitive, and each set A of imprimitivity is carried into itself by elements of G , i.e., there is a nontrivial partition Π of X such that $A \in \Pi$ implies $\varphi(A) = A$ for all $\varphi \in G$, so that $\varphi \in G$ is "nonmixing" on Π .

Consider a stage of switching that has N inlets and N outlets. It is evident that such a stage provides ways of connecting some of the inlets to some of the outlets. If the stage contains enough crosspoints it can be used to connect every inlet to some outlet in a one-to-one fashion, i.e., with no inlet connected to more than one outlet and vice versa. With the inlets and outlets both numbered $1, 2, \dots, N$, such a setting of the switches corresponds to a permutation on $\{1, \dots, N\}$. Indeed, there may be many ways of doing this, differing in what inlets are connected to what outlets, that is, corresponding to different permutations.

Definition 5: A stage S generates the permutation φ if there is a setting of N switches of S which connects each inlet to one and only one outlet in such a way that i is connected to $\varphi(i)$, $i = 1, \dots, N$, that is, if

$$(i, \varphi(i)) \in S.$$

Definition 6: The set of permutations generated by a stage S is denoted by $P(S)$.

Definition 7: A network (with N inlets and N outlets) generates a permutation φ if there is a setting of the switches in the network which connects, by mutually disjoint paths, each inlet to one and only one outlet in such a way that i is connected to $\varphi(i)$, $i = 1, \dots, N$.

If two stages S_1, S_2 are connected by a link pattern corresponding to a permutation φ_2 , then the permutations that they generate together are those of the form

$$\varphi_1 \varphi_2 \varphi_3, \quad \varphi_i \in P(S_i), \quad i = 1 \text{ or } 3.$$

If a network consists of two stages S_1, S_2 joined by a link pattern corresponding to a permutation φ , then it can be seen that it generates exactly the permutations in the set

$$P(S_1) \varphi P(S_2).$$

A network of s stages $S_i, i = 1, \dots, s$, with a link pattern corresponding to $\varphi_i, i = 1, \dots, s - 1$, between the i th and the $(i + 1)$ th stages, generates the complex

$$P(S_1)\varphi_1P(S_2) \cdots \varphi_{s-1}P(S_s).$$

We shall occasionally use the suggestive notation

$$S_1\varphi_1S_2 \cdots \varphi_{s-1}S_s$$

to refer to or indicate such a network.

It is now possible to formulate a group-theoretic approach to the analysis and synthesis of rearrangeable connecting networks made of stages of switching joined by link patterns. Consider such a network, generating the complex

$$P(S_1)\varphi_1 \cdots \varphi_{s-1}P(S_s).$$

The factors $\varphi_iP(S_{i+1}), i = 1, \dots, s - 1$, occurring herein are themselves again just complexes. Thus, given any product of complexes

$$\prod_{i=1}^s K_i$$

we seek to know whether the product is the whole symmetric group, and whether the factor complexes K_i can be written in the form

$$\varphi P(S)$$

where φ is a permutation and S is a stage. In this general form the problem is largely unsolved; however, special cases are worked out in the sequel.

V. THE GENERATION OF COMPLEXES BY STAGES

We start with this elementary result:

Remark 1: Let M be a complex (i.e., a set) of permutations. Define a stage S by

$$S = \{(x, y) : \varphi(x) = y \text{ for some } \varphi \in M\}.$$

Then $P(S) \supseteq M$ and no smaller stage has this property.

In cases of practical importance, such as shown in Figs. 1 and 2, the stages are made of square switches, and it is clear that a stage S (with N inlets and N outlets) is capable of effecting certain special permutations on $X = \{1, \dots, N\}$, and of course, all submaps thereof. (Indeed, for each switch there are numbers m and n with $m < n$ such that the switch

is capable of performing all the $(n - m + 1)!$ permutations of the numbers k in the range $m \leq k \leq n$ among themselves.) Since no inlet [outlet] is on more than one switch, these permutations form a *subgroup* of the symmetric group $S(X)$ of all permutations on $\{1, \dots, N\}$. This subgroup has a property which might be described intuitively by saying that there exist sets on which the subgroup elements can mix "strongly," but which they keep separate. It is apparent, indeed, that the subgroup generated by a stage made of square switches is strictly imprimitive, the sets of imprimitivity being just the elements of the partition Π of $\{1, \dots, N\}$ according to what switch an inlet [outlet] is on. This situation might also be described by saying that a permutation φ from the subgroup is *nonmixing* on Π .

Our second observation is

Remark 2: Let H be a strictly imprimitive group of permutations on $X = \{1, \dots, N\}$, with sets of imprimitivity forming the partition Π . Let S be the smallest stage with $P(S) \supseteq H$. Then

$$S = \bigcup_{A \in \Pi} A \times A,$$

i.e., S is made of square switches.

The main result of this section states that a stage can generate a subgroup only if it contains a substage made of square switches. This suggests that stages made of square switches necessarily arise in the generation of the symmetric group by products of complexes some of which are subgroups.

Theorem 1: Let S be a stage, and let $P(S)$ contain a subgroup H of $S(X)$. Then there is a substage \mathcal{R} of S which is made of square switches.

Proof: Define a relation \mathcal{R} on $\{1, \dots, N\}$ by the condition that $i\mathcal{R}j$ if and only if $j = \varphi(i)$ for some $\varphi \in H$. Since H is a subgroup, it must contain the identity permutation, i.e., $i\mathcal{R}i$ for all $i = 1, \dots, N$. Let i, j, k be numbers in $\{1, \dots, N\}$ such that $j = \varphi(i)$ and $k = \psi(j)$ for some permutations $\varphi, \psi \in H$. Then $\psi\varphi \in H$ and $k = \psi\varphi(i)$, that is, $i\mathcal{R}k$; hence \mathcal{R} is transitive. Finally, if $j = \varphi(i)$ with $\varphi \in H$, we have $i = \varphi^{-1}(j)$ with $\varphi^{-1} \in H$, since H is a group. Hence \mathcal{R} is an equivalence relation, and there is a partition Π such that

$$\mathcal{R} = \bigcup_{A \in \Pi} (A \times A).$$

Since $i\mathcal{R}j$ obviously implies $(i, j) \in S$, we have

$$\mathcal{R} \subseteq S.$$

\mathcal{R} is clearly a substage of S made of square switches.

VI. AN EXAMPLE

As is well-known, elementary group theory contains many results that allow one to write a group as a product of complexes. These results often involve a *subgroup* of the group in question. We shall quote an elementary result of this kind, and interpret it in terms of a network that is known to be rearrangeable.

Let G be a group, and let H_1 and H_2 be subgroups of G , not necessarily distinct. A *double coset* is a complex of the form

$$H_1\varphi H_2, \quad \varphi \in G$$

It is a known result⁵ that two double cosets are either identical or disjoint. Thus there is at least one complex M with the properties

$$\bigcup_{\varphi \in M} H_1\varphi H_2 = G$$

$$H_1\varphi H_2 \cap H_1\psi H_2 = \emptyset \quad \text{if } \varphi \neq \psi, \quad \text{with } \varphi, \psi \in M.$$

In particular

$$G = H_1 M H_2,$$

and we have factored G into a product of three complexes, two of which are subgroups. Now suppose that G is actually $S(X)$, the symmetric group of all permutations of N objects, and that m and n are positive integers such that $mn = N$. Let Π be a partition of $X = \{1, \dots, N\}$ into m sets of n elements each, and let H be the largest strictly imprimitive subgroup of $S(X)$ whose sets of imprimitivity form Π . Also let φ be a self-inverse permutation, and Π_φ a partition, such that $A \in \Pi, B \in \Pi_\varphi$ imply*

$$|\varphi(A) \cap B| = 1.$$

Let K be the largest strictly imprimitive subgroup of $S(X)$ whose sets of imprimitivity form Π_φ .

By Remark 2, Section IV, H and K can each be generated by stages of square switches.

Returning to the earlier discussion leading to the factorization $G = H_1 M H_2$, we let $H_1 = H_2 = H$. Now it can be seen that the complex

$$H\varphi K\varphi H$$

is generated by a network of the form shown in Fig. 2. By the Slepian-Duguid theorem (Beneš, Ref. 1, p. 1484) this network is rearrangeable, so that

$$H\varphi K\varphi H = S(X).$$

* $|A|$ denotes the number of elements of a set A .

Since $\varphi = \varphi^{-1}$, the complex $\varphi K \varphi$ is itself actually the subgroup $\varphi^{-1} K \varphi$ conjugate to K . Thus for $G = S(X)$ and $H_1 = H_2 = K$, the factor M in

$$S(X) = IIMH$$

can be chosen to be $\varphi^{-1} K \varphi$.

VII. SOME DEFINITIONS

The number of elements of a set A is denoted $|A|$. Let X, Y be arbitrary finite sets with $|X| = |Y|$, let B be a subset of Y , let Π_1, Π_2 be partitions of X, Y respectively, and let φ be a one-to-one map of Y onto X . Let θ be the null set.

Definition 8: $\varphi(B) = \{x \in X: \varphi^{-1}(x) \in B\}$.

Definition 9: φ hits Π_1 from B if and only if $A \in \Pi_1$ implies $\varphi(B) \cap A \neq \theta$.

Definition 10: φ covers Π_1 from Π_2 if and only if $B \in \Pi_2$ implies φ hits Π_1 from B .

Definition 11: $\varphi(\Pi_2)$ is the partition of X induced by φ acting on elements of Π_2 , i.e.,

$$\varphi(\Pi_2) = \{\varphi(B): B \in \Pi_2\}.$$

Definition 12: ${}_B\varphi$ is the restriction of φ to B .

Let A be a subset of X .

Definition 13: ${}_A\Pi_1$ is the partition of A induced by Π_1 , i.e.,

$${}_A\Pi_1 = \{C \cap A: C \in \Pi_1\}.$$

Definition 14: φ B -covers Π_1 from Π_2 if and only if ${}_B\varphi$ covers $\varphi(B)\Pi_1$ from ${}_B\Pi_2$.

Definition 15: Let Π_0, Π_1 be partitions of X . Then $\Pi_1 > \Pi_0$ (read "pi-one refines pi-zero") if and only if every set in Π_0 is a union of sets in Π_1 , and $\Pi_1 \neq \Pi_0$.

VIII. PRELIMINARY RESULTS

Lemma 1: Let X and Y be any sets with $|X| = |Y| < \infty$, let $\Pi_1 = \{A_1, \dots, A_n\}$ and $\Pi_2 = \{B_1, \dots, B_m\}$ be partitions of X and Y respectively, and suppose that for $k = 1, \dots, n$ the union of any k elements of Π_1 has more elements than the union of any $k - 1$ elements of Π_2 . Then

(i) $m \geq n$.

(ii) For each one-to-one map f of X onto Y there exists a set of n distinct integers $k(1), \dots, k(n)$ with $1 \leq k(i) \leq m, i = 1, \dots, n$, and

$$f(A_i) \cap B_{k(i)} \neq \emptyset \quad i = 1, \dots, n.$$

Proof: Since Π_1 and Π_2 are partitions, and $|X| = |Y|$,

$$\sum_{j=1}^n |A_j| = \sum_{j=1}^m |B_j|.$$

If m were less than n , then the union of m B 's has as many elements as the union of n A 's, for $m < n$; this contradicts the hypothesis. Let

$$K_i = \{j: f(l) \in B_j \text{ for some } l \in A_i\}, \quad i = 1, \dots, n.$$

Also let $A_{i(1)}, \dots, A_{i(k)}$ be any k elements of $\Pi_1, 1 \leq k \leq n$, and set

$$T = \bigcup_{j=1}^k K_{i(j)}.$$

All of the

$$\sum_{j=1}^k |A_{i(j)}|$$

elements of

$$\bigcup_{j=1}^k A_{i(j)}$$

are mapped by f into $|T|$ sets of Π_2 . Since no union of $k-1$ sets of Π_2 has

$$\sum_{j=1}^k |A_{i(j)}|$$

elements, it follows that $|T| \geq k$. Thus the union of any k of the sets $\{K_i, i = 1, \dots, n\}$ has at least k members. Hence by P. Hall's theorem⁶ there is a set of n distinct representatives $k(1), \dots, k(n)$ with

$$k(i) \in K_i \quad i = 1, \dots, n$$

$$k(i) \neq k(j) \quad \text{for } i \neq j.$$

But clearly $k(i) \in K_i$ if and only if

$$f(l) \in B_{k(i)} \quad \text{for some } l \in A_i,$$

that is, if and only if

$$f(A_i) \cap B_{k(i)} \neq \emptyset.$$

Lemma 2: Let Π_1, Π_2 be partitions of sets X, Y respectively with the properties $|X| = |Y|$ and

$$C_1, C_2 \in \Pi_1 \cup \Pi_2 \text{ implies } |C_1| = |C_2|.$$

Then for every one-to-one map φ of X onto Y there is a set $D \subseteq X$ such that φ hits Π_2 from D and φ^{-1} hits Π_1 from $\varphi(D)$.

Proof: We observe that $|\Pi_1| = |\Pi_2|$, and that the conditions of Lemma 1 are satisfied, with $m = n$. For each onto map φ there is a set $D \subseteq X$ with $|D| = |\Pi_1|$, such that

$$A \in \Pi_1 \text{ implies } D \cap A \neq \emptyset, \quad (\varphi^{-1} \text{ hits } \Pi_1 \text{ from } \varphi(D))$$

$$B \in \Pi_2 \text{ implies } \varphi(D) \cap B \neq \emptyset, \quad (\varphi \text{ hits } \Pi_2 \text{ from } D).$$

Lemma 3: Let X be any set and let Π_1 and Π_2 be partitions of X such that $A, B \in \Pi_1 \cup \Pi_2$ implies $|A| = |B|$. Then for every permutation φ on X there is a partition Π_φ of X such that (i) φ covers Π_2 from Π_φ , (ii) φ^{-1} covers Π_1 from $\varphi(\Pi_\varphi)$,

$$(iii) \quad |\Pi_\varphi| = |A|, \quad A \in \Pi_1 \cup \Pi_2$$

$$|B| = |\Pi_1| = |\Pi_2|, \quad B \in \Pi_\varphi.$$

Proof: Let φ be a permutation on X . The hypothesis implies that the union of any k elements of Π_1 has more elements than the union of any $k-1$ elements of Π_2 , for $k = 1, \dots, |\Pi_1|$. Hence by Lemma 2, with $X = Y$ and $m = n$, there is a set $D_1 \subseteq X$ such that

$$\varphi \text{ hits } \Pi_2 \text{ from } D_1$$

$$\varphi^{-1} \text{ hits } \Pi_1 \text{ from } \varphi(D_1).$$

Now we consider the sets $X_1 = X - D_1$ and $Y_1 = Y - \varphi(D_1)$ partitioned by

$${}_{X_1}\Pi_1 \quad \text{and} \quad {}_{Y_1}\Pi_2 \text{ respectively}$$

and we apply Lemma 2 to ${}_{X_1}\varphi$, i.e., to the restriction of φ to $X - D_1$. This gives a new set $D_2 \subseteq X$ such that again

$$\varphi \text{ hits } \Pi_2 \text{ from } D_2$$

$$\varphi^{-1} \text{ hits } \Pi_1 \text{ from } \varphi(D_2).$$

We proceed in this manner till X and Y are exhausted, and set $\Pi_\varphi = \{D_1, \dots, D_n\}$, where $n = |A|$ for all $A \in \Pi_1 \cup \Pi_2$. It is clear that Π_φ has the stated properties.

Let φ be a permutation on X , and let Π_1, Π_2 be partitions of X .

Lemma 4: If φ covers Π_1 from Π_2 , and $B \in \Pi_2$ implies $|B| = |\Pi_1|$, then $A \in \Pi_1$ implies $|A| = |\Pi_2|$.

Proof: Since φ covers Π_1 from Π_2 , then $A \in \Pi_1$ and $B \in \Pi_2$ imply that there is an $x \in B$ with $\varphi^{-1}(x) \in A$. Thus $\varphi^{-1}(x) \in A$ for at least $|\Pi_2|$ distinct values of x , and so $|A| \geq |\Pi_2|$. Since $B \in \Pi_2$ implies $|B| = |\Pi_1|$, it follows that $|\Pi_1|$ divides $|X|$ and

$$|\Pi_2| = \frac{|X|}{|\Pi_1|}.$$

Clearly

$$\sum_{A \in \Pi_1} |A| = |X|.$$

Since there are $|\Pi_1|$ sets in Π_1 each with at least $|\Pi_2|$ elements,

$$\sum_{A \in \Pi_1} |A| \geq |\Pi_1| \cdot |\Pi_2| = |X|.$$

If any $A \in \Pi_1$ had more than $|\Pi_2|$ elements the sum would exceed $|X|$, which cannot be. Thus $A \in \Pi_1$ implies $|A| = |\Pi_2|$.

IX. GENERATING THE PERMUTATION GROUP

In this section we exhibit a sufficient condition on permutations $\varphi_1, \dots, \varphi_{s-1}$ and stages S_1, \dots, S_s under which the complex

$$P(S_1)\varphi_1 \cdots \varphi_{s-1}P(S_s)$$

is actually the whole symmetric group, and the corresponding network (obtained by linking S_i and S_{i+1} by φ_i , $i = 1, \dots, s-1$) is rearrangeable.

In order to focus on the mathematical character of the results, on their purely formal aspects divorced from physical considerations having to do with switches, etc., the conditions on the φ 's and the S 's purposely are phrased in a quite abstract way. Consequently, the practical implications and applications of the result may be unclear and require discussion. This discussion is given after the theorem has been stated, and is followed by its proof.

Theorem 2: Let $s > 3$ be an odd integer, let $\varphi_1, \dots, \varphi_{s-1}$ be permutations on $X = \{1, \dots, N\}$, let Π_k , $k = 1, \dots, s$, and Π^k , $k = 1, \dots, \frac{1}{2}(s-1)$, be partitions of X , and let

$$\Psi^k = \begin{matrix} \{X\} & k = 0 \\ \varphi_k^{-1} \cdots \varphi_{\frac{1}{2}(s-1)}^{-1}(\Pi^k) & k = 1, \cdots, \frac{1}{2}(s-1) \\ \varphi_k \cdots \varphi_{\frac{1}{2}(s+1)}(\Pi^{s-k}) & k = \frac{1}{2}(s+1), \cdots, s-1, \\ \{X\} & k = s. \end{matrix}$$

Suppose that

- (i) If $s \geq 3$, then $\Pi^k < \Pi^{k+1}$, $k = 0, \cdots, \frac{1}{2}(s-3)$.
- (ii) $\Pi_{\frac{1}{2}(s+1)} = \Pi^{\frac{1}{2}(s-1)}$
- (iii) For $k = 1, \cdots, \frac{1}{2}(s-1)$, and every $B \in \Psi^{k-1}$, $\varphi_k^{-1} B$ covers Π_k from φ_k from $\varphi_k(\Psi^k)$.
- (iv) For $k = \frac{1}{2}(s+1), \cdots, s-1$, and every $B \in \Psi^{k+1}$, $\varphi_k B$ covers Π_{k+1} from $\varphi_k^{-1}(\Psi^k)$.
- (v) If $A \in \Pi^k$ and $B \in \Psi^{k-1} \cup \Psi^{k+\frac{1}{2}(s+1)}$ then $|{}_B \Pi_k| = |{}_B \Pi_{s-k+1}| = |A|$, $k = 1, \cdots, \frac{1}{2}(s-1)$.

Let H_k , $k = 1, \cdots, s$ be the largest strictly imprimitive subgroup of $S(X)$ whose sets of imprimitivity are exactly the elements of Π_k (i.e., $A \in \Pi_k$ implies $\{ {}_A \varphi: \varphi \in H_k \} = S(A)$). Then the complex K defined by

$$K = H_1 \varphi_1 H_2 \cdots H_{s-1} \varphi_{s-1} H_s$$

has the property $K = S(X)$, and any network generating this complex is rearrangeable.

The theorem given above does not provide any new designs of rearrangeable networks that are not already implicit in the work of M. C. Paull³ and D. Slepian,¹ thus no new principle is involved. Rather, in formulating the result, we have sought insight by stating a generalized, purely combinatorial form of these previous results. The theorem exhibits this generalization, first as providing a way of generating the symmetric group in a fixed number of multiplications of certain restricted group elements, and second as based on some purely abstract properties of some partitions and permutations.

As in A. M. Duguid's proof of the Slepian-Duguid theorem,¹ the basic combinatorial theorem of P. Hall on distinct representatives of subsets is used repeatedly. This means (roughly) that the proof proceeds by showing that an arbitrary permutation (to be realized in the network) can be decomposed into submaps each of which can be realized in a disjoint part of the network, thereby not interfering with the realization of the other submaps. A significant departure from Ref. 3 is that we try to obtain rearrangeability directly from conditions that are stated for the network as a whole, as well as by building it up from rearrangeable subnetworks.

The following intuitive guides should be useful in understanding

Theorem 2. The permutations $\varphi_1, \dots, \varphi_{s-1}$ are of course intended to be those corresponding to the link patterns between the stages of a network. The partition Π_k corresponds to the assignment of the terminals entering the k th stage to various square switches, all $u \in A$ for $A \in \Pi_k$ being on the same switch. The partitions Π^k are used in defining the submaps mentioned above.

The "covering" properties (iii) and (iv) of the φ_k in Theorem 2 ensure (roughly) that the φ_k are sufficiently mixing or distributive to be able to generate all permutations in the restricted ways permitted in the definition of K . They are generalizations of the property, exhibited in Fig. 2, that every middle switch is connected to every side switch by a link. The property (v), finally, implies that various sets of switches all have the same cardinality; this ensures (again, roughly) that if a cross-point is not being used for a connection between one inlet-outlet pair, then it can be used for a connection between some other pair.

Proof of Theorem 2: We use induction on odd $s \geq 3$. If $s = 3$, there is only one Π^k , viz. Π^1 . Let φ be a permutation; we show that

$$\varphi \in H_1 \varphi_1 H_2 \varphi_2 H_3.$$

The argument to be given is constructive, in that we do not use proof by contradiction, but actually give a kind of recipe for finding three permutations $\eta_i \in H_i$, $i = 1, 2, 3$, with

$$\varphi = \eta_1 \varphi_1 \eta_2 \varphi_2 \eta_3.$$

To prove the theorem for $s = 3$, it is enough for $i = 1, 2, 3$ to exhibit a partition $\Pi(i)$ and to define η_i on $A \in \Pi(i)$, i.e., to give

$$A \eta_i, \quad A \in \Pi(i), \quad i = 1, 2, 3.$$

Condition (v) for $k = 1$ ($= \frac{1}{2}(s - 1)$ here) tells us that for $A \in \Pi^1$

$$|\Pi_1| = |\Pi_3| = |A|.$$

However, the "middle-stage" condition (ii) states that $\Pi_2 = \Pi^1$. Hence $|\Pi_1| \cdot |\Pi_2| = N$. Since [condition (iii) now] φ_1^{-1} covers Π_1 from $\varphi_1(\Pi^1) = \varphi_1 \varphi_1^{-1}(\Pi^1) = \Pi_2$, it follows that $B \in \Pi_1$ implies $|B| \geq |\Pi_2|$. If for some $B \in \Pi_1$ it was true that $|B| < |\Pi_2|$, then

$$\sum_{B \in \Pi_1} |B| < |\Pi_1| \cdot |\Pi_2| = N$$

which is impossible. Thus $|B| = |\Pi_2|$ for $B \in \Pi_1$. In exactly the same way, using condition (iv), we find that $C \in \Pi_3$ implies $|C| = |\Pi_2|$. Therefore $B, C \in \Pi_1 \cup \Pi_3$ implies $|B| = |C|$.

Returning now to the chosen permutation φ , we apply Lemma 3 to conclude that there exists a partition Π_φ of X such that φ covers Π_3 from Π_φ , φ^{-1} covers Π_1 from $\varphi(\Pi_\varphi)$, $|\Pi_\varphi| = |A|$ for $A \in \Pi_1 \cup \Pi_3$, and $|B| = |\Pi_1| = |\Pi_3|$ for $B \in \Pi_\varphi$. Hence also $|\Pi_\varphi| = |\Pi_2|$.

Let $\mu: \Pi_\varphi \leftrightarrow \Pi_2$ be any map of Π_φ onto Π_2 . The desired partitions $\Pi(i)$, $i = 1, 2, 3$ will be taken to be

$$\Pi(1) = \varphi_1(\Pi_2)$$

$$\Pi(2) = \{\mu(D) : D \in \Pi_\varphi\} = \Pi_2$$

$$\Pi(3) = \Pi_\varphi$$

and the desired permutations η_i , $i = 1, 2, 3$, are defined so as to have these properties: for $D \in \Pi_\varphi$

$$\eta_3 : \varphi(D) \leftrightarrow \varphi_2^{-1}(\mu(D))$$

$$\eta_1 : \varphi_1(\mu(D)) \leftrightarrow D$$

$$\eta_2 : \varphi_2\eta_3(D) \leftrightarrow \varphi_1^{-1}\eta_1^{-1}\varphi(D).$$

That this can be done (uniquely, indeed) can be seen as follows: Let $D \in \Pi_\varphi$, and $\mu(D) = B \in \Pi_2$. Since φ^{-1} covers Π_1 from $\varphi(\Pi_\varphi)$, and φ covers Π_3 from Π_φ , it must be true that

(1) φ^{-1} hits Π_1 from $\varphi(D)$

(2) φ hits Π_3 from D .

But at the same time, by conditions (iii) and (iv), and the fact that $\Pi^1 = \Pi_2$, φ_1^{-1} covers Π_1 from Π_2 and φ_2 covers Π_3 from Π_2 , and so

(3) φ_1^{-1} hits Π_1 from B

(4) φ_2 hits Π_3 from B .

Thus if $u \in D \cap A$ and $A \in \Pi_3$, there is a unique $v \in A$ such that $\varphi_2(v) \in B$, and we take $\eta_3(u) = v$. Similarly, if $z = \varphi(u) \in C$ and $C \in \Pi_1$, there is a unique $w \in C$ such that $\varphi_1^{-1}(w) \in B$, and we take $\eta_1(w) = z$. Finally, define η_2 so that $\eta_2(\varphi_2(v)) = \varphi_1^{-1}(w)$. Since $\mu(\cdot)$ is onto, each $D \in \Pi_\varphi$ deals with a unique $B = \mu(D) \in \Pi_2$, and the definition of η_i , $i = 1, 2, 3$ can be made for each D and its associated B , independently of the others. It is apparent that

$$\eta_1\varphi_1\eta_2\varphi_2\eta_3(D) = \varphi(D), \quad D \in \Pi_\varphi,$$

or

$$\varphi = \eta_1\varphi_1\eta_2\varphi_2\eta_3.$$

Since η_i for $i = 1, 2, 3$ is onto, and is a subset of

$$\bigcup_{E \in \Pi_i} E \times E,$$

it follows that $\eta_i \in H_i$, $i = 1, 2, 3$, and thus that

$$K = S(X).$$

We now assume, as an hypothesis of induction, that the theorem is true for a given odd $s - 2 \geq 3$, and that we are given permutations φ_k , and partitions $\{\Pi_k\}$ and $\{\Pi^k\}$, satisfying the conditions of the theorem.

No loss of generality is sustained if it is assumed that each $A \in \Pi^2$ is invariant under $\varphi_2, \dots, \varphi_{s-2}$. This invariance can always be achieved by redefining the φ_i , without loss of properties (iii) to (v). It can now be seen that for $k = 2, \dots, s - 2$ the restrictions

$${}_A\Pi_k, \quad {}_A\Pi^k, \quad \text{with } A \in \Pi^2,$$

satisfy all the conditions on Π_k, Π^k (respectively) used in Theorem 2. Hence by the hypothesis of induction, for each $A \in \Pi^2$, the restriction of the complex

$$H_2\varphi_2 \cdots \varphi_{s-2}H_{s-1}$$

to A generates $S(A)$. The argument used for the case $s = 3$ can now be used to complete the induction, $\Psi^2 (= \Psi^{s-1}$ here) playing the role of Π_2 .

X. CONSTRUCTION OF A CLASS OF REARRANGEABLE NETWORKS

We consider a network ν built of an odd number $s \geq 3$ of stages,

$$\nu = S_1\varphi_1 \cdots \varphi_{s-1}S_{s-1},$$

satisfying the symmetry conditions

$$\left. \begin{aligned} \varphi_k &= \varphi_{s-k}^{-1} \\ S_k &= S_{s-k+1} \end{aligned} \right\} k = 1, \dots, \frac{1}{2}(s-1),$$

with each stage S_k made of identical square switches. The φ_k will be chosen in the following way: order the switches of each stage; to define φ_k for a given $1 \leq k \leq \frac{1}{2}(s-1)$ take the first switch of S_k , say with n outlets and n a divisor of N , and connect these outlets one to each of the first n switches of S_{k+1} ; go on to the second switch of S_k and connect its n outlets one to each of the next n switches of S_{k+1} ; when all the switches of S_{k+1} have one link on the inlet side, start again with the first switch; proceed cyclically in this way till all the outlets of S_k are assigned. (See Fig. 3.)

We shall show that a network ν constructed in this way is always rearrangeable.

Theorem 3: Let $s \geq 3$ be an odd integer. Let $n_k, k = 1, \dots, (s+1)/2$, be any positive integers such that

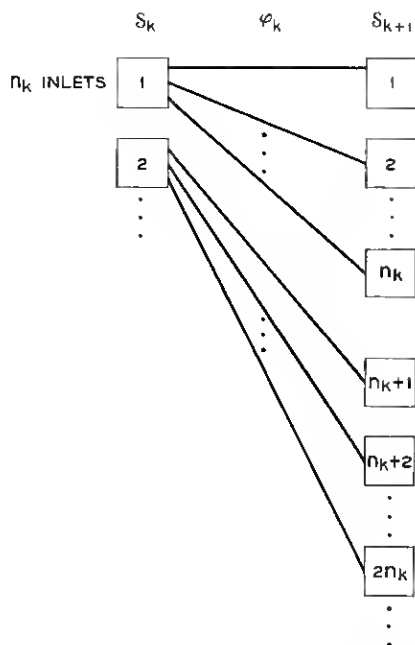


Fig. 3 — Assignment of inlets and outlets of rearrangeable network.

$$\prod_{i=1}^{s+1} n_i = N \quad \text{and} \quad n_i \geq 2.$$

For each $k = 1, \dots, (s+1)/2$, let Π_k be the partition of $X = \{1, \dots, N\}$ into the N/n_k sets of the form

$$A_{ki} = \{t: (i-1)n_k < t \leq in_k\} \quad i = 1, \dots, N/n_k.$$

Let $\varphi_k, k = 1, \dots, (s-1)/2$, be permutations with the property that $n \equiv t \pmod{N/n_{k+1}}$ if and only if

$$\varphi_k(n) \in A_{k+1,t} \quad t = 0, \dots, (N/n_{k+1}) - 1.$$

Define

$$\varphi_k = \varphi_{s-k}^{-1} \quad \text{for} \quad (s-1)/2 < k \leq s-1.$$

Let $S_k, k = 1, \dots, s$, be the stages made of square switches defined by

$$S_k = S_{s-k+1} \quad k = 1, \dots, (s-1)/2$$

$$S_k = \bigcup_{A \in \Pi_k} A \times A$$

and ν be the network constructed by putting a link pattern corresponding to φ_k , $k = 1, \dots, s-1$ between stages S_k and S_{k+1} . Then ν is rearrangeable.

Proof: It is readily seen that for $k = 1, \dots, s$

$$\begin{aligned} P(S_k) &= \text{the largest strictly imprimitive subgroup with sets of im-} \\ &\quad \text{primitivity } \Pi_k, \\ &= H_k, \end{aligned}$$

in the notation of Theorem 2. Thus to prove the theorem by appeal to Theorem 2 it is enough to exhibit suitable partitions Π^k , $k = 1, \dots, \frac{1}{2}(s-1)$, and to show that these, together with $\varphi_1, \dots, \varphi_{s-1}$, satisfy the conditions of Theorem 2. For $k = 1, \dots, \frac{1}{2}(s-1)$, set

$$\begin{aligned} \Pi^k &= \text{class of all } \{j: (i-1)N/n_1 \cdots n_k < j \leq iN/n_1 \cdots n_k, \\ &\quad i = 1, \dots, n_1 n_2 \cdots n_k\}. \end{aligned}$$

It is evident that the Π^k are successively finer partitions, i.e., that

$$\Pi^k < \Pi^{k+1} \quad k = 1, \dots, \frac{1}{2}(s-3).$$

Also, since $\Pi^{\frac{1}{2}(s-1)}$ consists of the $n_1 n_2 \cdots n_{\frac{1}{2}(s-1)}$ sets

$$\{j: (k-1)n_{\frac{1}{2}(s+1)} < j \leq kn_{\frac{1}{2}(s+1)}, k = 1, \dots, n_1 n_2 \cdots n_{\frac{1}{2}(s-1)}\}$$

it can be seen that

$$\Pi^{\frac{1}{2}(s-1)} = \{A_{\frac{1}{2}(s+1), i} : 1 \leq i < N/n_{\frac{1}{2}(s+1)}\},$$

and hence that the middle stage condition (ii) in Theorem 2,

$$\Pi_{\frac{1}{2}(s+1)} = \Pi^{\frac{1}{2}(s-1)},$$

is satisfied.

The remainder of the proof, in which the requisite covering properties of the φ_k are demonstrated, is based on some auxiliary results.

Lemma 5: For $k = 2, \dots, \frac{1}{2}(s-1)$, and $1 \leq i \leq N/n_k n_{k+1}$ the following identity holds

$$\bigcup_{\substack{t \equiv i-1 \\ (\text{mod } \frac{N}{n_k n_{k+1}})}} A_{k,t} = \varphi_k^{-1} \left(\bigcup_{i-1 < \frac{t}{n_k} \leq i} A_{k+1,t} \right)$$

and the sets on the right are disjoint for different i .

Proof: Since

$$\varphi_k^{-1}(A_{k+1,t}) = \{n: n \equiv t \pmod{N/n_{k+1}}, \quad 1 \leq n \leq N\}$$

the union on the right in the lemma is the set of all n that are $\equiv t \pmod{N/n_{k+1}}$

N/n_{k+1} for some l with $(i-1)n_k < l \leq in_k$. Consider such an n , with say

$$n = \frac{lN}{n_{k+1}} + t, \quad \begin{array}{l} i-1 < \frac{l}{n_k} \leq i \\ 0 \leq t < n_{k+1}. \end{array}$$

Then

$$n = n_k \frac{lN}{n_k n_{k+1}} + (i-1)n_k + u,$$

with $0 < u \leq n_k$, and so

$$n \in A_{k, (lN/(n_k n_{k+1}) + i - 1)}$$

or

$$n \in A_{k, l} \quad \text{with} \quad l \equiv (i-1) \pmod{N/n_k n_{k+1}}.$$

Since the representation of n in terms in l and u is unique, the lemma follows.

The practical or physical import of the lemma is this: In any stage $k+1$, $1 \leq k \leq \frac{1}{2}(s-1)$, the i th block of n_k switches is connected by the link pattern φ_k to exactly those n_{k+1} switches (in the k th stage) whose number $l \equiv (i-1) \pmod{N/n_k n_{k+1}}$.

Definition: For $1 \leq i \leq n$, and $2 \leq k \leq m = \frac{1}{2}(s+1)$

$$B_{ik} = \bigcup_t \left\{ A_{k, t} : t \equiv r \pmod{n_1 n_2 \cdots n_{k-1}} \text{ for some } r \text{ with } (i-1) < \frac{r}{n_2 n_3 \cdots n_{k-1}} \leq i \right\}$$

where $n_2 n_3 \cdots n_{k-1}$ is taken = 1 if $k = 2$.

Lemma 6: For $1 \leq i \leq n_1$ and $2 \leq k < m$

$$B_{ik} = \varphi_k^{-1}(B_{i, k+1}).$$

Proof: We show that the right-hand side contains the left. Equality then follows from Lemma 5, since $B_{i, k+1}$ will always be a union of sets of the form

$$\bigcup_{j-1 < \frac{r}{n_k} \leq j} A_{k+1, r}.$$

This is because $t \equiv r \pmod{u}$ if and only if $t + 1 \equiv (r + 1) \pmod{u}$, if $0 \leq r < u$. Consider then an $n \in B_{ik}$. There is a $t \geq 1$ congruent to an $r \pmod{n_1 n_2 \cdots n_{k-1}}$, with

$$i - 1 < \frac{r}{n_2 n_3 \cdots n_{k-1}} \leq i,$$

such that $n \in A_{k,t}$. The latter fact implies that

$$(t - 1)n_k < n \leq tn_k.$$

Now $\varphi_k(n) \in A_{k+1,\gamma}$, where n is congruent to $\tau \pmod{N/n_{k+1}}$, so we can represent n in the form

$$n = \frac{aN}{n_{k+1}} + \tau.$$

Hence

$$(t - 1)n_k < \frac{aN}{n_{k+1}} + \tau \leq tn_k.$$

Writing $t = ln_1 n_2 \cdots n_{k-1} + r$, with

$$(i - 1)n_2 n_3 \cdots n_{k-1} < r \leq in_2 n_3 \cdots n_{k-1},$$

we see that

$$qn_1 \cdots n_k + (r - 1)n_k < \tau \leq qn_1 \cdots n_k + rn_k$$

where

$$q = l - \frac{aN}{n_1 n_2 \cdots n_{k+1}}.$$

It follows that τ is congruent $\pmod{n_1 n_2 \cdots n_k}$ to some integer p in the region

$$(i - 1)n_2 \cdots n_k < p \leq in_2 \cdots n_k,$$

and thus $\varphi_k(n) \in B_{i,k+1}$, completing the proof of Lemma 6.

Now if $k = m$, the defining condition that $t \equiv r \pmod{n_1 \cdots n_{m-1}}$ for some r with

$$(i - 1)n_2 \cdots n_{m-1} < r \leq in_2 \cdots n_{m-1},$$

used in the definition of B_{ik} , can be put into a slightly different form. In this case we must have

$$1 \leq t \leq N/n_m = n_1 n_2 \cdots n_{k-1}$$

and so t can only be congruent to r by being equal to r , that is

$$(i - 1)n_2 \cdots n_{m-1} < t \leq in_2 \cdots n_{m-1}.$$

Hence it can be seen that

$$\{B_{im}, i = 1, \cdots, n_1\} = \Pi^1.$$

Applying Lemma 6 ($m - 2$) times we find that

$$\begin{aligned}\{B_{i2}, i = 1, \cdots, n_1\} &= \varphi_2^{-1} \cdots \varphi_m^{-1}(\Pi^1) \\ &= \varphi_1(\Psi^1).\end{aligned}$$

Now $n \equiv t \pmod{N/n_2}$ if and only if $\varphi_1(n) \in A_{2t}$, $t = 1, \cdots, N/n_2$. Also, by definition of B_{i2} ,

$$B_{i2} = \bigcup_{t \equiv i \pmod{n_1}} A_{2t}.$$

Let $\varphi_1(n) \in B_{i2}$, $\varphi_1(n) \in A_{2t}$. Then n has the form

$$n = \frac{aN}{n_1 n_2} n_1 + t = \left(\frac{aN}{n_1 n_2} + b \right) n_1 + i,$$

so $n \equiv i \pmod{n_1}$. Since $|B_{i2}| = |B_{im}| = n_2 \cdots n_m = N/n_1$, it follows that B_{i2} is the φ_1 image of N/n_1 integers each of which is congruent to $i \pmod{n_1}$. Since each such integer must be in a different A_{1t} , it follows that φ_1^{-1} covers Π_1 from $\varphi_1(\Psi^1)$.

The remaining conditions in Theorem 3 can be demonstrated in essentially the same way; one has merely to identify the sets in question, and use Lemma 5 and an analog of Lemma 6. The details will be omitted.

REFERENCES

1. Beneš, V. E., On Rearrangeable Three-Stage Connecting Networks, B.S.T.J., **41**, 1962, pp. 1481-1492.
2. Beneš, V. E., Optimal Multistage Rearrangeable Connecting Networks, B.S.T.J., this issue, p. 1641.
3. Paull, M. C., Reswitching of Connection Networks, B.S.T.J., **41**, May, 1962, pp. 833-855.
4. Hall, M., Jr., *The Theory of Groups*, Macmillan, New York, 1959, p. 64.
5. *Ibid.*, p. 10.
6. Hall, P., On Representatives of Subsets, J. London Math. Soc., **10** (1935), pp. 26-30.